

CLAIMS

What is claimed is:

1. A method for detecting spoofed network connections comprising:
receiving a connection from a client;
delaying sending a greeting message for a delay period;
monitoring the connection during the delay period; and
if a command is received from the client before the greeting is sent, then identifying the connection as a possible spoofed connection.
2. The method of claim 1 further comprising:
sending the greeting to the client upon completion of the delay period.
3. The method of claim 1 further comprising:
processing any electronic mail associated with a spoofed connection.
4. The method of claim 3 wherein electronic mail associated with a spoofed connection is processed using a process selected from the group consisting of:
deleting a spoofed-connection electronic mail message;
marking a spoofed-connection electronic mail message; and
storing a spoofed-connection electronic mail message in a special electronic directory.
5. The method of claim 1 wherein the connection is a Transmission Control Protocol (TCP) connection.
6. The method of claim 1 wherein the client is a Mail Transfer Agent (MTA) or Mail User Agent (MUA).
7. The method of claim 1 wherein the received command is a Simple Mail Transfer Protocol (SMTP) command.

8. A method for detecting spoofed network connections comprising:
receiving a first command at a server from a client;
delaying, for a delay period, a transmission of a reply associated with the first command;
monitoring a connection between the server and the client during the delay period; and
if a second command is received at the server before the reply is transmitted, then
identifying the connection as a possible spoofed connection.

9. The method of claim 8 further comprising:
sending a greeting to the client when the connection is established with the server.

10. The method of claim 8 further comprising:
transmitting the reply upon completion of the delay period.

11. The method of claim 8 further comprising:
processing any electronic mail associated with the spoofed connection.

12. The method of claim 8 wherein the connection is a Transmission Control Protocol (TCP) connection.

13. The method of claim 8 wherein the client is a Mail Transfer Agent (MTA) or Mail User Agent (MUA).

14. The method of claim 8 wherein the received command is a Simple Mail Transfer Protocol (SMTP) command.

15. An apparatus for detecting spoofed connections comprising:
means for detecting when a connection is established between the apparatus and a client device;
means for transmitting a greeting message or a reply or both to the client device;
means for delaying the transmitting means so that the greeting message or the reply or both are not transmitted during a delay period; and
means for monitoring the connection to detect commands that are sent by the client device at least during the delay period.

16. The apparatus of claim 15 wherein the client device is a Mail Transfer Agent (MTA) or Mail User Agent (MUA).

17. The apparatus of claim 15 wherein the detecting means, the transmitting means, the delaying means, and the monitoring means comprise one or more processor-based devices running software algorithms to provide the detecting, transmitting, delaying and monitoring functions.

18. The apparatus of claim 15 wherein the connection is a Transmission Control Protocol (TCP) connection.

19. The apparatus of claim 15 wherein the commands are Simple Mail Transfer Protocol (SMTP) commands.